Disaster Recovery

Disaster Recovery Roundtable Test

On December 18, 2015 [Bank Personnel] including [List Participants] conducted a roundtable testing.

Scenario: On [Date], an overnight fire has occurred at the bank’s main location rendering the facility unusable. Critical server assets were subject to overheating and found to be unusable as well.

Scenario: On [Date], a tornado warning was issued with bank personnel taking shelter. The main lobby and offices were hit and are unusable. Critical server assets remain intact; however, communication (Internet and phone lines) are all down; the respective vendors anticipate a minimum of 72 hours before communications can be restored.

Scenario: On [Date], following heavy snowfall and extreme cold temperatures, bank personnel are unable to make it in to the main location, as well as all branch locations. Based on weather forecasts, anticipated service outage is between 24 and 48 hours.

Scenario: On [Date], bank personnel began reporting unusual activity on computers including random files deleting and extremely slow network activity. Internet connectivity to the bank has been disconnected with the network support vendor reporting all critical server assets compromised. New server equipment and a full refresh of all devices is required with an indefinite period of network downtime.

The purpose of the roundtable testing exercise was to test the bank’s ability to recover necessary resources (network, core, facilities, etc.) within either established recovery locations or in the main location itself, as well as to test the bank’s ability to continue to provide banking services to its customers.

Discussion items:

* [List items read and reviewed]

Follow up items are as follows.

1. [List follow up items]

Employees Attended